



Autorité de protection des données
Gegevensbeschermingsautoriteit

(Verleende) machtiging nr. 001/2026 van 16 februari 2026

Betreft: machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: "Command-and-Control" (C2) - waarschuwingen – 2 (AH-2025-0072)

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* (hierna "de WOG");

Gelet op artikel 21, § 4, van de wet van 26 april 2024 *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "de NIS2-wet");

Gelet op de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna "de WEC");

Gelet op Verordening (EU) 2016/679 *van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "de AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "de WVG");

Gelet op de artikelen 44, 54 en 55 van het Reglement van interne orde van de Gegevensbeschermingsautoriteit (hierna "het RIO");

Gelet op de machtigingsaanvraag van de directeur-generaal van het Centrum voor Cybersecurity België, de heer Miguel De Bruycker (hierna "de aanvrager"), ontvangen op 13 november 2025;

Gelet op de machtiging van de Autoriteit nr. 001/2025 van 18 juli 2025 *betreffende een machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: "Command-and-Control servers communicatiemetadata – waarschuwing" (AH-2025-0034)*, opgenomen in de bijlage 2;

Gelet op het verzoek om aanvullende informatie dat op 24 november 2025 aan het Centrum voor Cybersecurity België is gericht;

Gelet op de aanvullende informatie die op 21 januari 2026 door het Centrum voor Cybersecurity België is verstrekt;

Gelet op de bevestiging van de volledigheid van het dossier die op 4 februari 2026 aan de aanvrager is verzonden;

Neemt op 16 februari 2026 de volgende beslissing:

I. Voorwerp en context van de machtigingsaanvraag

1. De aanvrager heeft bij de Autoriteit een machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de NIS2-wet ingediend (hierna "**de aanvraag**"). Deze aanvraag staat rechtstreeks in verband met machtiging nr. 001/2025 van 18 juli 2025 van de autoriteit *betreffende een machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: "Command-and-Control servers communicatiemetadata — waarschuwing" (AH-2025-0034)* (hierna "**machtiging nr. 001/2025**", opgenomen in bijlage 2) **en valt binnen het toepassingsgebied daarvan**. De Autoriteit verwijst naar machtiging nr. 001/2025 ter inleiding en ter toelichting van de onderhavige aanvraag. Het gaat om een project van de aanvrager waarbij deze contact opneemt met de slachtoffers van C2-servers na de analyse van elektronische-communicatiemetagegevens die zijn verzameld bij Belgische verstrekkers van elektronische-communicatienetwerken (operatoren) (hierna: "**het project**" van de aanvrager). **De onderhavige machtiging moet worden gelezen in samenhang met machtiging nr. 001/2025.**
2. De aanvrager heeft bij zijn aanvraag (geclassificeerd als "GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)", "TLP: AMBER+STRICT") de volgende **vier bijlagen** (samen "**de documentatie**") gevoegd, waarnaar hierna wordt verwezen:

- ■ hierna de “**projectnota**”, geclassificeerd als “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)”, “TLP: AMBER+STRICT”;
 - ■ hierna de “**interne procedure**”, geclassificeerd als “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)”, “TLP: AMBER+STRICT”;
 - ■ hierna de “**methodenota**”, geclassificeerd als “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)”, “TLP: AMBER+STRICT”;
 - ■ hierna de “**lijst van C2S**”, geclassificeerd als “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)”, “TLP: AMBER+STRICT”;
3. Wat de **indeling van de bijlagen** betreft, vermeldt het CCB in de projectnota het volgende: “*Alle documenten die door het CCB in het kader van dit project worden geproduceerd, zijn geclassificeerd als “GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)” - TLP:AMBER+STRICT.*” De Autoriteit neemt hiervan kennis en **houdt hiermee rekening, mits de betreffende documenten de relevante vermelding daadwerkelijk bevatten**. Wat de publicatie van de onderhavige machtiging betreft, moet de aanvrager de Autoriteit **binnen de 10 werkdagen** vanaf de kennisgeving van deze beslissing (de datum van verzending van de e-mail van de Autoriteit aan de aanvrager geldt als bewijs – de Autoriteit benadrukt dat deze termijn strikt moet worden nageleefd) duidelijk aangeven welke passages van haar beslissing volgens haar niet mogen worden gepubliceerd op grond van de door haar aangevoerde redenen (**overwegingen 6-11 van machtiging nr. 001/2025**)¹.
4. Via de aanvraag wordt in wezen het volgende gevraagd: toegang tot nieuwe elektronische communicatiemetagegevens en de voor deze toegang benodigde machtiging, middels een aanpassing van bepaalde voorwaarden die zijn vastgelegd in machtiging nr. 001/2025, rekening houdend met aanvullende elementen en modaliteiten die in het project zijn vastgelegd (wijzigingen aan het oorspronkelijke project).

II. Onderzoek

De onderhavige beslissing is als volgt gestructureerd en bevat een bijlage:

II.1. Wijzigingen aan de oorspronkelijke aanvraag met betrekking tot de context van machtiging nr. 001/2025 en de aanpak die in het kader van onderhavige machtiging is gevolgd.....	4
II.2. Uitbreiding van de aanvraag wat betreft de betrokken metagegevens.....	5
II.2.1. Met betrekking tot de soorten betrokken metagegevens.....	5
II.2.2. Wat betreft de betrokken operatoren (Belnet, Telenet en Proximus)	7

¹ Deze oefening is uiteraard niet nodig voor de bijlage 2.

II.2.3. Wat betreft de betrokken elektronische communicatie (communicatie uit het verleden, artikelen 122 en 123 van de WEC)	8
II.4. Uitbreiding van de aanvraag met betrekking tot het nagestreefde doeleinde en de verdere gegevensverwerkingen?	13
II.5. Gebruik van alternatieve maatregelen om op te treden tegen C2-servers.....	18
II.6. Controle of een IP-adres wel degelijk uitsluitend bestemd is en blijft voor de activiteiten van een C2-server	21
II.6.1. Uitgevoerde controles.....	21
II.6.2. Wijziging van de controlefrequentie van IP-adressen	21
II.7. Beperking van de contextuele informatie die aan de operatoren wordt verstrekt	22
II.8. Bewaartermijn van de gegevens.....	24
II.9. Rechten van de betrokkenen	25
II.10. Wettelijke grondslag voor de verwerking en wijziging van het bestaande normatieve kader .	26
II.11. Beslissing	28



II.1. Wijzigingen aan de oorspronkelijke aanvraag met betrekking tot de context van machtiging nr. 001/2025 en de aanpak die in het kader van onderhavige machtiging is gevolgd

5. Hoewel de door de aanvrager verstrekte documentatie met betrekking tot het project aangepast is, is het niet altijd evident om de nuances van de aanvraag duidelijk te onderscheiden ten opzichte van wat door de Autoriteit is goedgekeurd in haar machtiging nr. 001/2025. De aanvrager verwijst ook niet naar de relevante overwegingen in machtiging nr. 001/2025 die, op de een of andere manier in het licht van zijn aangepaste ontwerp, problematisch zouden zijn.

6. **De onderhavige machtiging mag niet worden opgevat als een validatie van de door de aanvrager verstrekte documentatie. De aanvrager moet duidelijk en expliciet aangeven welke relevante overwegingen in een machtiging van de Autoriteit op de een of andere manier problemen kunnen geven in het kader van zijn project en naar zijn mening een aanpassing van de door de Autoriteit gevolgde aanpak vereisen.** Het is echter ook aan hem om **aan te geven waarom een dergelijke aanpassing noodzakelijk is** voor het goede vervolg van zijn project. Als hij dat niet doet, moet de Autoriteit de documenten vergelijkend lezen, wat tot fouten, onbegrip en inefficiëntie leidt. De Autoriteit herinnert eraan dat zij in deze zaak gebonden is aan een bijzonder strikte beslissingstermijn, die weliswaar wordt opgeschort tijdens de voorbereiding van het dossier.

7. Dit gezegd zijnde, **staat de Autoriteit positief tegenover de gevolgde aanpak van de aanvrager om, rekening houdend met de wijzigingen in zijn project, een voorafgaande machtigingsaanvraag in te dienen**, in plaats van - ervan uitgaande dat in het kader van zijn aanvraag een beroep op dringendheid zou kunnen worden gedaan - de Autoriteit voor een voldongen feit te plaatsen in een situatie van controle achteraf. Een dergelijke benadering garandeert een efficiëntere en juridisch gezien veiligere werkwijze.
8. Op basis van de verstrekte aanvraag en documentatie **merkt de Autoriteit op dat de volgende aspecten van het gewijzigde project van de aanvrager een reactie en, indien nodig, een specifieke beslissing vereisen ten aanzien van machtiging nr. 001/2025:**
- De uitbreiding van de aanvraag wat betreft de soorten van betrokken metagegevens;
 - De uitbreiding van de aanvraag naar twee andere operatoren (Proximus en Telenet);
 - De uitbreiding van de aanvraag tot elektronische-communicatiemetagegevens die in het verleden hebben plaatsgevonden (toegang tot elektronische-communicatiemetagegevens die door de operatoren worden bewaard);
 - De mogelijke uitbreiding van de aanvraag met betrekking tot het nagestreefde doeleinde en de verdere gegevensverwerking;
 - De kwestie van het gebruik van alternatieve maatregelen om op te treden tegen C2-servers (blokkering, melding aan de gerechtelijke autoriteiten en via Threat Alerts);
 - De aanpassing van de regelmaat waarmee het CCB (nationaal CSIRT) controleert of een IP-adres nog steeds uitsluitend wordt gebruikt voor de activiteiten van een C2-server;
 - De beperking van de contextuele informatie die aan de operatoren wordt verstrekt;
 - De rechten van betrokkenen.
9. De Autoriteit heeft zich ook grondiger gebogen over **bepaalde technische aspecten** van het project van de aanvrager.
10. Al deze onderwerpen worden in de verdere uiteenzettingen behandeld.

II.2. Uitbreiding van de aanvraag wat betreft de betrokken metagegevens

II.2.1. Wat betreft de soorten betrokken metagegevens

11. Uit de door de aanvrager verstrekte documentatie blijkt dat voortaan "*indien mogelijk, andere **beschikbare metagegevens***", worden beoogd █ (in vet aangeduid en onderstreept door de Autoriteit). De Autoriteit vroeg de aanvrager om deze overige metagegevens nauwkeurig en uitvoerig te identificeren en aan te tonen dat ze noodzakelijk zijn in het kader van zijn project. Hij antwoordde het volgende:

“Met deze passage uit de interne procedure wordt bedoeld dat aan de ISPs gevraagd zou worden om minstens een minimale set metadata te delen ■ Deze vraag zou, mits autorisatie door de GBA, afdwingbaar zijn. **Daarnaast echter, nodigen we ISPs immer uit om andere metadata te delen, indien mogelijk en beschikbaar, en daarom dus ook niet verplichtend of afdwingbaar, en ondergeschikt aan hun eventuele wettelijke beperkingen alsook technische mogelijkheden en beschikbare capaciteit.** Indien dit in de ogen van de GBA te ver gaat, kunnen we dit uit onze verzoeken aan de ISP's verwijderen.

12. Dit antwoord geeft aanleiding tot de twee volgende opmerkingen. Enerzijds herinnert de Autoriteit eraan dat volgens artikel 2, 93°, van de WEC, “elektronische-communicatiemetagegevens” worden gedefinieerd als “de gegevens die worden **verwerkt** in een elektronische-communicatienetwerk **met het oog op de transmissie, de distributie of de uitwisseling van de inhoud van elektronische communicatie**, met inbegrip van gegevens waarmee een communicatie kan worden getraceerd en de bron en de bestemming van de communicatie kunnen worden bepaald, alsmede gegevens betreffende de locatie van de apparatuur die in het kader van het aanbieden van elektronische-communicatiediensten zijn gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie” (in vet aangeduid door de Autoriteit). Zonder dat de Autoriteit de analyse hierover voortzet, lijken de voornoemde gegevens echter niet noodzakelijk te zijn voor de transmissie van de betreffende communicatie, maar veeleer aanvullende statistische/geaggregeerde gegevens te zijn met betrekking tot de betreffende individuele communicatie.
13. Anderzijds, **en nog fundamentele**, deelt de Autoriteit het standpunt van de aanvrager dat het in artikel 21, § 2, van de NIS2-wet bedoelde geval betrekking heeft op een **verplichting** van operatoren om de betrokken gegevens te verstrekken. In dit **eerste geval**, zoals de Autoriteit overigens al heeft verduidelijkt, zijn beide entiteiten – enerzijds de operator en anderzijds het CCB (nationaal CSIRT) – afzonderlijke verwerkingsverantwoordelijken. De eerste is verantwoordelijk voor de communicatie van gegevens aan het CCB (nationaal CSIRT) krachtens een wettelijke verplichting die is vastgelegd in de NIS2-wet en die op hem van toepassing is, en de tweede is verantwoordelijk voor een gegevensverwerking die noodzakelijk is voor de uitvoering van haar taken van algemeen belang zoals vastgelegd in diezelfde wet.
14. Het **tweede geval**, waarin de operator **vrijwillig zou besluiten** gegevens uit te wisselen met het CCB (nationaal CSIRT), is juridisch gezien aanzienlijk verschillend en roept bijkomende vragen op (Wat met de wettelijke basis en de rechtmatigheid van de mededeling van gegevens door de operator in deze context?; Wat met de aansprakelijkheden van de operatoren en het CCB (nationaal CSIRT) met betrekking tot alle uitgevoerde gegevensverwerkingen – worden zij in dit geval *gezamenlijke* verwerkingsverantwoordelijken voor de betreffende verwerkingen?; enz.). **In ieder geval is de Autoriteit niet bevoegd om deze kwesties in het kader van de onderhavige aanvraag te**

behandelen, en zeker niet om zich uit te spreken over dit tweede scenario van gegevensverwerking aangezien dit volgens haar buiten het toepassingsgebied van artikel 21, § 2, van de NIS2-wet valt.

15. De Autoriteit heeft zich bovendien afgevraagd wat de verwijzing naar **ruwe gegevens**, met betrekking tot de door de operatoren verstrekte gegevens, voor de aanvrager betekende ("CCB ontvangt liefst ruwe gegevens als beschikbaar maar kan eventueel werken op geaggregeerde gegevens"). De aanvrager antwoordde het volgende:

"Ruwe data zoal Pcaps (of dus Full Packet Capture) – indien ze beschikbaar zijn en (zowel legaal als technisch) kunnen/mogen gedeeld worden – kunnen immer meer informatie geven en analyses verrijken mbt het type en schaal van aanval. Geaggregeerde metadata is echter ook reeds voldoende om eerste analyses uit te voeren om te verifiëren dat het effectief gaat om kwaadaardig verkeer met Belgische slachtoffers en hen te waarschuwen. Verdere analyse op ruwere data kan vervolgens uitgevoerd worden in samenspraak met het slachtoffer."(in vet aangeduid door de Autoriteit)

16. Naast het voorgaande met betrekking tot wat door de operatoren kan of moet worden meegedeeld, bevestigt de Autoriteit dat het **in het kader van het project en de onderhavige machtiging onwettig is om bij operatoren Pcap-gegevens (packet capture) te verzamelen**, voor zover dergelijke gegevens met name betrekking hebben op de **inhoud van elektronische communicatie** (bevatten), hetgeen per definitie en dus duidelijk verder gaat dan het begrip elektronische-communicatiemetagegevens zoals vermeld in overweging 12.

II.2.2. Wat betreft de betrokken operatoren (Belnet, Telenet en Proximus)

17. De aanvraag betreft de toegang tot elektronische-communicatiemetagegevens die door **Belnet, Telenet en Proximus** worden verwerkt. Deze laatste twee operatoren waren niet betrokken bij machtiging nr. 001/2025. Met name gelet op de non-discriminatievereiste zoals vastgelegd in artikel 21, § 1, van de NIS2-wet, heeft de Autoriteit de aanvrager gevraagd naar de reden waarom zijn aanvraag is uitgebreid (en slechts is uitgebreid) tot Telenet en Proximus, aangezien de Autoriteit er vanaf het begin van uitging dat Belnet een zodanig specifiek karakter had, in verband met de soorten organisaties die tot haar klantenkring behoren (overheidsdiensten, ziekenhuizen, enz.), dat de opname ervan geen vragen oproep. De aanvrager antwoordde het volgende (vrije vertaling):

"Alleen Proximus, Telenet en Belnet vallen onder de aanvraag, aangezien we al eerste contacten hebben kunnen leggen met deze drie operatoren. We weten dat deze operatoren bereid zijn om in het kader van het onderhavige project met het CCB samen te werken. Zo

kunnen we de uitvoering van het project in een tweede fase richten op operatoren die met ons willen samenwerken, wat de lancering ervan vergemakkelijkt. Met deze drie operatoren weten we dat de samenwerking vruchtbaar zal zijn en dat het project hierdoor op termijn nog verder in positieve zin kan worden ontwikkeld, voordat het wordt uitgebreid naar andere operatoren.”

18. De Autoriteit neemt akte van dit antwoord. De Autoriteit wijst het CCB (nationaal CSIRT) erop, aangezien er andere operatoren dan Belnet bij betrokken zijn, dat het voor het bereiken van haar doelstellingen van belang is toe te zien op de naleving van de beginselen van objectiviteit en non-discriminatie, overeenkomstig **artikel 21, § 1, van de NIS2-wet**. Rekening houdend met het doeleinde van het ontwerp, dat erop gericht is ernstige bedreigingen aan te pakken en alle soorten entiteiten te helpen zich hiertegen te beveiligen, **is het de taak van het CCB (nationaal CSIRT) om er tevens op toe te zien dat de geografische dekking van het project en de dekking wat betreft de infrastructuur van openbare elektronische-communicatienetwerken in België relevant en coherent zijn**. De Autoriteit benadrukt bovendien het belang van het **delen van informatie over C2-servers** via de gebruikelijke kanalen van het CCB (nationaal CSIRT), wat in dit geval des te belangrijker is voor de operatoren en entiteiten die niet onder het toepassingsgebied van het project vallen². Tijdige en betrouwbare informatie over C2-servers en de IP-adressen die zij gebruiken, maakt het ook mogelijk om het aantal potentiële slachtoffers te beperken.

II.2.3. Wat betreft de betrokken elektronische communicatie (communicatie uit het verleden, artikelen 122 en 123 van de WEC)

19. *"De aanvraag heeft enerzijds betrekking op de communicatiemetagegevens die door de betrokken operator worden bewaard vanaf de datum van deze machtigingsaanvraag, zolang de betrokken IP-adressen zijn toegewezen aan de betrokken C2-servers, en anderzijds op de communicatiemetagegevens **die door de betrokken operator vóór de datum van onderhavige machtigingsaanvraag zijn bewaard overeenkomstig de in de artikelen 122 en 123 van de WEC genoemde termijnen, wanneer uit de gegevens waarover het CCB beschikt, kan worden vastgesteld dat er sprake was van eerdere kwaadwillige activiteiten** "* (onderstreping verwijderd en in vet aangeduid en vertaald door de Autoriteit)³
20. De aanvrager wil op deze manier toegang krijgen tot **elektronische-communicatiemetagegevens die in het verleden zijn opgeslagen**. Voor elk IP-adres wordt in de verstrekte documentatie een **"first seen"-datum** vermeld, vanaf welke datum de door de operatoren bewaarde metagegevens moeten worden verstrekt. Dit betekent dat de aanvraag interageert met de regels inzake de bewaring

² Zie met name de overwegingen 45-47.

³ Punt 6 van de aanvraag.

van metagegevens door de operatoren, met inbegrip van en in het bijzonder de **wetgeving die van toepassing is op de verplichte bewaring van elektronische-communicatiemetagegevens** door deze entiteiten⁴. Dit onderwerp heeft aanleiding gegeven tot verschillende arresten van het Hof van Justitie van de Europese Unie⁵ en recentelijk tot **arrest nr. 97/2024 van het Grondwettelijk Hof** van 26 september 2024, waarin het Hof onder meer prejudiciële vragen (nog steeds in behandeling) heeft gesteld aan het Hof van Justitie van de Europese Unie.

21. Uit de aanvraag van het CCB (nationaal CSIRT) blijkt dat het toegang wenst te krijgen tot de **gegevens zoals bedoeld in de artikelen 122 en 123 van de WEC**:

- De **§§ 2 en 3 van artikel 122 staan** operatoren **toe** om “verkeersgegevens” betreffende de abonnees of eindgebruikers te verwerken voor bepaalde eigen doeleinden, namelijk in wezen: de facturering van abonnees, interconnectiebetalingen, bepaalde marketingdoeleinden en het aanbieden van diensten op basis van verkeers- of locatiegegevens;
- **Artikel 122, § 4, van de WEC** beoogt een **verplichting** tot de bewaring van gegevens door de operatoren, teneinde fraude of kwaadwillig gebruik van het netwerk of de dienst vast te stellen of de dader of de herkomst ervan te identificeren;
- **Artikel 122, § 4/1, van de WEC** bepaalt op zijn beurt dat de operatoren bepaalde gegevens **mogen** bewaren om de veiligheid en correcte werking van hun elektronische-communicatienetwerken en -diensten te garanderen, en in het bijzonder om een mogelijke of werkelijke aanslag op die veiligheid op te sporen en te analyseren, inclusief om de oorsprong van deze aanslag te identificeren;
- Ten slotte bepaalt **artikel 123 van de WEC** dat de operatoren van mobiele netwerken in een aantal gevallen andere locatiegegevens dan verkeersgegevens met betrekking tot een

⁴ Overeenkomstig artikel 127/1, § 5, tweede lid, van de WEC, laat de bevoegde minister “in het Belgisch Staatsblad een omzendbrief publiceren die een lijst omvat met de Belgische autoriteiten die gemachtigd zijn om van een operator gegevens te ontvangen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 en 127” en een dergelijke omzendbrief werd gepubliceerd in het *Belgisch Staatsblad* van 1 maart 2024, p. 29298, ook beschikbaar via <https://www.bipt.be/operatoren/publicatie/omzendbrief-over-de-toegang-van-de-autoriteiten-tot-de-gegevens-bewaard-door-de-operatoren>, laatst geraadpleegd op 25/11/2025. Het BIPT publiceerde ook een “Fiche voor het CCB” op haar website, zie <https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/c3fab97d608b2ff8135e949bb9cad24cb49709f/10-fiche-voor-het-centrum-voor-cybersecurity-belgie.pdf>, laatst geraadpleegd op 25/11/2025. De Autoriteit spreekt zich hier niet uit over de inhoud van deze documenten.

⁵ HvJ-EU (Grote kamer), arrest van 20 september 2022, *Bundesrepublik Deutschland tegen SpaceNet AG, Telekom Deutschland GmbH*, gevoegde zaken C-793/19 en C-794/19; HvJ-EU (Grote kamer), arrest van 5 april 2022, *G.D. tegen Commissioner of the Garda Síochána e.a.*, zaak C-140/20; HvJ-EU (Grote kamer), arrest van 6 oktober 2020, *La Quadrature du Net*, gevoegde zaken C-511/18, C-512/18 en C-520/18; HvJ-EU (Grote kamer), arrest van 21 december 2016, *Tele2 Sverige*, gevoegde zaken C-203/15 en C-698/15; HvJ-EU (Grote Kamer), arrest van 8 april 2014, *Digital Rights Ireland*, gevoegde zaken C-293/12 en C-594/12.

abonnee of eindgebruiker mogen bewaren, met name wanneer dat noodzakelijk is voor de goede werking en de veiligheid van het netwerk of van de dienst (**§ 1, 1°**), of wanneer dat noodzakelijk is om fraude of kwaadwillig gebruik van het netwerk op te sporen of te analyseren (**§ 1, 2°**).

22. In het kader van het beroep dat bij het Grondwettelijk Hof is ingesteld tegen de wet van 20 juli 2022 *betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten*⁶, heeft het Grondwettelijk Hof **prejudiciële vragen** gesteld aan het Hof van Justitie, met name over artikel 5, 4° en 5°, van deze wet, bepalingen die de huidige **paragrafen 4 en 4/1 van artikel 122 van de WEC**⁷ invoegen, en over artikel 6, voor zover dit voorziet in de huidige **§ 1, 1° en 2°, van artikel 123, van de WEC**⁸. Met andere woorden, **de bepalingen waarnaar in de laatste drie leden van overweging 21 wordt verwezen, vormen het voorwerp van prejudiciële vragen die momenteel door het Hof van Justitie worden onderzocht.**

23. In deze context heeft de Autoriteit de aanvrager een aantal vragen gesteld om: te verifiëren hoe ver de voornoemde zaak bij het Hof van Justitie was gevorderd en of er een beoordeling was uitgevoerd van de impact ervan op zijn project; vast te stellen hoe lang de betrokken operatoren (Proximus, Telenet en Belnet) de opgezochte elektronische-communicatiemetagegevens voor hun eigen doeleinden bewaren; en te begrijpen hoe (volgens welke procedure en op welke grondslag) de “*first seen*”-datums worden vastgesteld⁹. Ten slotte, aangezien in de projectnota het volgende wordt vermeld: “*Bij ernstige incidenten blijkt bovendien vaak dat de inbreuk vele maanden soms jaren aanwezig was alvorens gedetecteerd te worden*”, heeft de Autoriteit de aanvrager gevraagd of hij over cijfers op dit gebied beschikte. De aanvrager antwoordde het volgende:

■
 “Het CCB kan hierover geen details of structurele cijfers vrijgeven”
 ■

24. De Autoriteit neemt derhalve kennis van het feit dat **de datum “first seen” de oudste bevestigde datum is waarop een verband is vastgesteld tussen de betrokken activiteit van de bedoelde C2-server en het betrokken IP-adres waarop de aanvraag betrekking heeft.**

⁶ Het arrest wordt geciteerd in overweging 19.

⁷ Zie B.23 en B.32.

⁸ Zie B.33.1., B.35.3, B.39.2 en B.39.3.

⁹ ■

25. Het is **echter** aan de aanvrager om zijn documentatie, en meer bepaald de methodenota, aan te passen zodat de datum die als “*first seen*” wordt aangenomen, **overeenkomt met een concrete gebeurtenis.** ■
26. Wat betreft de bewaartermijn van de metagegevens voor de eigen doeleinden van de operatoren en de stand van zaken in de **bij het Hof van Justitie aanhangige zaak** en de beoordeling van de impact daarvan op het project, heeft de aanvrager het volgende geantwoord (vrije vertaling):

*“Wij **hebben geen kennis van de bewaartermijn van de metagegevens bij de betrokken operatoren voor hun eigen doeleinden.** Ons project is **uitsluitend gebaseerd op de gegevens die de operatoren wettelijk verplicht zijn te bewaren in het kader van de WEC.**”* (in vet aangeduid door de Autoriteit)

***“De zaak is momenteel nog aanhangig bij het Hof van Justitie (HvJ-EU). Het advies van de advocaat-generaal is nog niet uitgebracht.”** [De informatie is hier te vinden.](#) De Europese Commissie, de lidstaten en de verzoekers hebben schriftelijke opmerkingen geformuleerd. Het CCB heeft kennis kunnen nemen van arrest nr. 97/2024 van het Grondwettelijk Hof van 26 september 2024 en het bij de vaststelling ervan kunnen analyseren, en er nota van genomen dat het Hof de wet van 20 juli 2022 in dit stadium niet nietig verklaart. Dat leek al een belangrijk punt te zijn in vergelijking met hoe het Grondwettelijk Hof de vorige wet uit 2016 had beoordeeld. Overigens maakt het mechanisme voor toegang tot categorieën van elektronische-communicatiegegevens (afhankelijk van het doeleinde van de bewaring) door de bevoegde autoriteiten geen deel uit van de prejudiciële vragen die in de zaak C-661/24 aan het HvJ-EU zijn voorgelegd.*

De mogelijke impact heeft voornamelijk betrekking op de eventuele bewaring van gegevens van elektronische communicatie door de operatoren, met het oog op de bestrijding van fraude en het kwaadwillig gebruik van het netwerk of de dienst (met inbegrip van de identificatie van de daders en de herkomst). Indien het HvJ-EU overweegt dat het in het Belgische recht vastgelegde bewaarmechanisme voor de voornoemde doeleinden in strijd is met het Unierecht, zou dit kunnen leiden tot een beperktere bewaring van gegevens waartoe het CCB toegang vraagt.

Dit gezegd zijnde, stellen noch het arrest nr. 97/2024 van het Grondwettelijk Hof, noch de prejudiciële vragen die aan het HvJ-EU zijn voorgelegd, de toegangsmogelijkheden tot categorieën van elektronische-communicatiegegevens (afhankelijk van het doeleinde van de bewaring ervan) ter discussie in het kader van de doeleinden zoals bedoeld in artikel 21, § 1 en § 2, tweede lid, van de wet van 26 april 2024 tot vaststelling van een kader voor de

cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2-wet). Hoewel de impact van de gegevens waartoe het CCB in voorkomend geval toegang kan hebben niet te verwaarlozen is, is deze niet van dien aard dat het optreden van het CCB op het gebied van de toegang tot bepaalde elektronische-communicatiegegevens voor doeleinden – die altijd van niet-strafrechtelijke aard zijn – zoals de preventie, het onderzoeken en opsporen van strafbare feiten die online of via een elektronische-communicatienetwerk of -dienst zijn gepleegd, het voorkomen van ernstige bedreigingen voor de openbare veiligheid, en het onderzoeken van tekortkomingen in de beveiliging van elektronische-communicatienetwerken of -diensten of van informatiesystemen.” (in het vet aangeduid door de Autoriteit)

27. Het is aan de aanvrager om **in het kader van het project een procedure in te voeren die waarborgt dat hij zo snel mogelijk rechtstreeks de nodige maatregelen treft in het kader van zijn project naar aanleiding van het komende arrest van het Hof van Justitie**. De Autoriteit benadrukt in deze context het belang van de vraag die aan de aanvrager is gesteld over de bewaartermijn van elektronische-communicatiemetagegevens door de operatoren **voor hun eigen doeleinden** (een vraag waarop de aanvrager geen antwoord kon geven). Op dit moment en juridisch gezien levert de toegang tot de metagegevens die door de operatoren worden verwerkt op grond van de **paragrafen 2 en 3 van artikel 122** geen probleem op.
28. Onder deze voorwaarden **mogen** elektronische-communicatiemetagegevens voorafgaand aan de datum van de onderhavige beslissing **alleen worden verzameld op basis van de** door het CCB (nationaal CSIRT) **vastgestelde “first seen”-datums** (zie de methodenota en bijlage 1) **indien aan de volgende vier voorwaarden is voldaan:**
- De metagegevens worden verzameld op basis van **precieze wettelijke grondslagen** (artikel en naargelang het geval, paragraaf, lid, punt en nummer) die expliciet en duidelijk door het CCB (nationaal CSIRT) aan de operatoren worden aangegeven (het CCB nationaal CSIRT mag zich op dit punt niet beperken tot een algemene verwijzing naar de artikelen 122 en 123 van de WEC);
 - De metagegevens worden **door de betrokken operatoren wettelijk bewaard**, overeenkomstig de artikelen 122 en 123 van de WEC, afhankelijk van de wettelijke grondslag van de aanvraag;
 - De aanvrager zet een procedure op om **in het kader van zijn project direct rekening te houden met de verwachte uitspraak van het Hof van Justitie**: hij moet de

rechtmatigheid van de verwerking van metagegevens in het kader van het project op basis van die uitspraak opnieuw beoordelen en daaruit de nodige conclusies trekken;

- Elke bijgehouden “*first seen*”-datum wordt in de door de aanvrager bewaarde documentatie gekoppeld aan een concrete gebeurtenis die wijst op een **verband tussen de betrokken activiteit van de C2-server waarop de aanvraag betrekking heeft en het betrokken IP-adres. Indien deze datum te ver in het verleden ligt** met betrekking tot de wettelijk toegestane bewaartermijnen voor metagegevens door de operatoren, **moet** de datum van de metagegevens die mogen worden verzameld **dienovereenkomstig worden aangepast in de documentatie van de aanvrager**. De Autoriteit wijst de aanvrager hierop, met name wat betreft ■

II.4. Uitbreiding van de aanvraag met betrekking tot het nagestreefde doeleinde en de verdere gegevensverwerkingen?

29. Met betrekking tot het doeleinde van de aanvrager bepaalt de aanvraag het volgende: “*Het project (zie projectfiche in bijlage) heeft betrekking op de identificatie en de waarschuwing van slachtoffers (met inbegrip van NIS2-entiteiten, overheidsinstanties, bedrijven, burgers, enz.) van C2-servers in verhouding tot de wettelijke doelstellingen (zoals de opsporing van inbreuken die online of via een netwerk of een elektronische communicatiedienst worden gepleegd (zonder strafrechtelijke finaliteit) – de waarschuwing van potentiële slachtoffers en de preventie van ernstige bedreigingen voor de openbare veiligheid).*” De projectnota lijkt echter verder te gaan dan wat de Autoriteit op basis van het oorspronkelijke project heeft toegestaan in de overwegingen 25 en 29 van machtiging nr. 001/2025: “*Hel doel van het CCB-project en het daaropvolgende verzoek om toegang tot elektronischecomunicatiemetagegevens bij operators van elektronische communicatie is enerzijds het Informeren van de beheerders van informatiesystemen die het slachtoffer zijn van C2-servers, zodat zij de nodige maatregel kunnen nemen om zich te beschermen, en anderzijds het onderzoeken van tekortkomingen in de beveiliging van netwerken en informatiesystemen*” (vetgedrukt gewijzigd door de Autoriteit). Deze nota gaat evenwel verder als volgt: “*Deze doelstellingen vloeien voornamelijk voort uit de taak van het nationale CSIRT zoals vastgelegd in artikel 19, § 1, 2°, van de NIS2-wet. Het gaat erom waarschuwingen en informatie over cyberdreigingen en kwetsbaarheden te verspreiden onder potentiële slachtoffers, indien mogelijk in bijna-realtime. Op die manier heeft het project een preventief effect op de uitvoering van dreigingen en schade bij de doelwitten van de C2-servers[...]. Voor de uitvoering ervan is het noodzakelijk om tekortkomingen in de beveiliging van elektronische communicatienetwerken en informatiesystemen te onderzoeken, d.w.z. het opsporen, observeren en analyseren van IT-beveiligingsproblemen die verband houden met de betrokken bedreigingen.*” (vetgedrukt gewijzigd door de Autoriteit)

30. Op basis van deze voorwaarden heeft de Autoriteit de aanvrager gevraagd te bevestigen dat de overwegingen 25 en 29 van machtiging nr. 001/2025 nog steeds actueel zijn in het kader van zijn project en, indien dit niet het geval is, wat er concreet opnieuw zou worden overwogen. De aanvrager antwoordde het volgende (vrije vertaling):

"De overwegingen 25 en 29 van de machtiging zijn nog steeds volledig actueel. Dit deel van het project met betrekking tot het doel van het project benadrukt vooral de overwegingen van de Autoriteit in punt 29, namelijk:

1. *"Het betreft het verspreiden van meldingen en informatie over cyberdreigingen en kwetsbaarheden onder potentiële slachtoffers, indien mogelijk in real time."*; en
2. *"Voor de uitvoering ervan is het noodzakelijk beveiligingsgebreken bij elektronische-communicatienetwerken en informatiesystemen te onderzoeken (artikel 21, § 2, 3°, van de NIS2-wet). Dit omvat het opsporen, observeren en analyseren van computerbeveiligingsproblemen die verband houden met de betrokken dreigingen."*

We hebben de overwegingen van de Autoriteit rechtstreeks in de nieuwe versie van ons project opgenomen." (in vet aangeduid door de Autoriteit)

31. De Autoriteit neemt kennis van dit antwoord en benadrukt dat het project inderdaad **slechts één doeleinde** nastreeft, namelijk het verspreiden van meldingen en informatie over cyberdreigingen en kwetsbaarheden onder potentiële slachtoffers, indien mogelijk in real time. Het onderzoek naar de in dit kader noodzakelijke tekortkomingen ("*En anderzijds het onderzoeken van...*") vormt geen afzonderlijk doeleinde van de verwerking van elektronische-communicatiemetagegevens, maar maakt wel deel uit van het voornoemde doeleinde. De daarmee samenhangende verwerkingsactiviteiten zijn inderdaad noodzakelijk om de aanvrager in staat te stellen het doeleinde van het project te verwezenlijken.
32. Deze vragen kunnen in verband worden gebracht met het onderwerp van de **verdere verwerking van de gegevens** die in het kader van de aanvraag zijn verzameld. Twee passages uit het ontwerp kunnen in dit verband vragen oproepen: "*Zo mogen de analyses op basis van de verzamelde metagegevens niet worden doorgegeven voor toezicht, incidentrespons of strafrechtelijke vervolging, **tenzij wettelijk anders bepaald***" (in vet aangeduid door de Autoriteit) – wat zijn de andere gevallen?; "*Gegevens die ouder zijn dan een jaar worden door een geautomatiseerd systeem vernietigd, **onverminderd de resultaten van het onderzoek en de rapporten** die door het CCB zijn opgesteld in het kader van het **onderzoek** naar de C2-servers dat is gestart nadat communicatie tussen deze servers en slachtoffers was vastgesteld.*" (in vet aangeduid door de Autoriteit) – Bevatten deze resultaten en rapporten dan ook elektronische-communicatiemetagegevens en is het gebruiksdoel ervan wel dusdanig beperkt dat het contact opnemen met de betrokken slachtoffers

gerechtvaardigd is? Zo niet, hoe zit het dan? Op vragen hierover antwoordde de aanvrager het volgende (vrije vertaling):

*"Deze passage in het project heeft namelijk tot doel elke verdere verwerking van de gegevens uit te sluiten, tenzij dit op grond van een toepasselijke wettelijke bepaling vereist is. **We bedoelen hier met name artikel 29 van het Wetboek van Strafvordering**, dat ons kan verplichten tot de verdere verwerking van de gegevens die wij ontvangen in het kader van onze wettelijke verplichting om strafbare feiten aan de gerechtelijke autoriteiten te melden. Deze passage is in ons project opgenomen om tegemoet te komen aan de overwegingen die de Autoriteit in punt 105 van haar machtiging had gemaakt, namelijk: "[...] de in het kader van het project verzamelde metagegevens mogen met andere woorden niet verder worden verwerkt voor andere doeleinden dan die welke door het project worden beoogd (met inbegrip van uiteraard de verwerkingen in verband met de toepassing van de rechtsregels die op het project zelf van toepassing zijn) [...]." (in vet aangeduid door de Autoriteit)*

"Met rapporten wordt ten eerste bedoeld: de waarschuwings- en adviesrapporten die aan de slachtoffers zouden worden gestuurd. Deze zullen de nodige elementen bevatten om elk slachtoffer apart correct te informeren over de aanval die we bij hen vaststelden en hoe deze kan gemitigeerd worden. Bijvoorbeeld: het CCB stelde tussen moment X en Y malware Z vast op poorten A en B van een aan jullie behorend IP-adres C. Dit zullen nooit de ruwe metadata-gegevens zijn.

*Anderzijds zullen ook rapporten opgesteld worden **ter informeren van de andere veiligheidsdiensten, waarin informatie op geaggregeerde wijze zal verwerkt worden om trends vast te stellen, volgens onze samenwerkingsverplichtingen bepaald in artikel 25, § 2, van de NIS2-wet en in artikel 20, § 1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.***

Tot slot zullen er ook rapporten aan de bevoegde procureur des Konings overgemaakt worden volgens de wettelijke verplichtingen waarin vastgestelde inbreuken worden gemeld, met alle informatie die relevant is voor het onderzoek (zie ook vraag 5.2.1)." (in vet aangeduid door de autoriteit)

33. De Autoriteit herhaalt vooreerst ten aanzien van de aanvrager de overweging 105 van haar machtiging nr. 001/2025: *"De Autoriteit herinnert er vooreerst aan dat de normatieve bepalingen die de bij haar ingediende machtigingsaanvraag regelen, in het bijzonder artikel 21, § 4, van de NIS2-wet en artikel 23, § 3, van de WOG, een specifiek normatief dispositief vormen (een lex specialis en bovendien een lex posterior) voor de toegang tot metagegevens van elektronische communicatie die door de operatoren worden verwerkt. De in het kader van het project verzamelde metagegevens mogen met andere woorden niet verder worden verwerkt voor andere doeleinden dan die welke door het project*

worden beoogd (**met inbegrip van uiteraard de verwerkingen in verband met de toepassing van de rechtsregels die op het project zelf van toepassing zijn**). Elke verdere verwerking voor andere doeleinden zou in strijd zijn met de Belgische wetgeving inzake de toegang tot metagegevens van elektronische communicatie die door de operatoren in het kader van hun activiteiten worden verwerkt¹⁰." (vetgedrukt en onderstreping aangepast door de Autoriteit in het kader van onderhavige machtiging) Met de in vet aangeduide zin doelde de Autoriteit bovenal op de regels die het project zelf regelen, zoals de daarvoor geldende regels inzake gegevensbescherming, waarvan de uitvoering een verdere verwerking van elektronische-communicatiemetagegevens kan vereisen (bijvoorbeeld om de rechtmatigheid of onrechtmatigheid van een gegevensverwerking aan te tonen).

34. In het kader van het ontwerp merkt de Autoriteit op dat de toepassing van **artikel 29 van het Wetboek van Strafvordering**¹¹ tot op zekere hoogte in tegenspraak lijkt te zijn met het doeleinde van het project zelf en met de bedoelingen van de aanvrager. Wat dit laatste punt betreft, bestaat de door de aanvrager gevolgde aanpak uit ■¹². Het oorspronkelijke doel kan hier niet zijn om bewijsmateriaal te verzamelen ten behoeve van strafrechtelijke procedures. Deze mogelijke tegenstrijdigheid komt des te duidelijker naar voren wanneer het project wordt bekeken in het licht van de netwerkmonitoring die in de nationale strategie inzake cyberveiligheid¹³ wordt voorzien, het feit dat de ambtenaren van het CCB (nationaal CSIRT) blijkbaar niet aan het beroepsgeheim¹⁴ zijn gebonden en de mogelijkheid om het project op termijn uit te breiden naar "Belgische" C2-servers¹⁵. Deze tegenstrijdigheid komt tot uiting in de bewoordingen van artikel 21, § 2, derde lid, van de NIS2-wet, die (*lex posterior* ten opzichte van artikel 29 van het Wetboek van Strafvordering) betrekking heeft op: "**zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten.**" (in vet aangeduid door de Autoriteit) Een systematische toepassing van artikel 29 van het Wetboek van Strafvordering in een dergelijke context (normatief, het project en de nationale strategie inzake cyberveiligheid) zou in de praktijk de reikwijdte van deze

¹⁰ "Zie in dezelfde zin (verleende) machtiging nr. 001/2024 van 6 november 2024 *betreffende een machtigingsaanvraag zoals bedoeld in artikel 15, § 2, tweede lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (AH-2024-0010)*, overweging nr. 76."

¹¹ Artikel 29, § 1, van het Wetboek van Strafvordering luidt als volgt:

"Iedere gestelde overheid, ieder openbaar officier of ambtenaar en, voor de sector van de gezinsbijslag, iedere meewerkende instelling in de zin van de wet van 11 april 1995 tot invoering van het handvest van de sociaal verzekerde die in de uitoefening van zijn ambt kennis krijgt van een misdaad of van een wanbedrijf, is verplicht daarvan dadelijk bericht te geven aan de procureur des Konings bij de rechtbank binnen wier rechtsgebied die misdaad of dat wanbedrijf is gepleegd of de verdachte zou kunnen worden gevonden, en aan die magistraat alle desbetreffende inlichtingen, processen-vertaal en akten te doen toekomen."

¹² ■

¹³ Zie over dit punt het advies van de Autoriteit nr. 69/2025 *met betrekking tot de "Nationale Cybersecurity Strategie 3.0, 2026-2030" (CO-A-2025-108)*, overwegingen 11-15.

¹⁴ Het beroepsgeheim staat de toepassing van artikel 29 van het Wetboek van Strafvordering in de weg; zie in dit verband met name GwH, arrest 44/2019 van 14 maart 2019, B.5.4.

¹⁵ Zie het antwoord van de aanvrager, aangehaald in overweging 55 van machtiging nr. 001/2025:

"[...] Het zou echter mogelijk zijn om dit element in een tweede fase van het project opnieuw te evalueren en ook servers die in België gevestigd zijn, op te nemen [...]"

beperking ("zonder strafrechtelijke finaliteit") aanzienlijk kunnen verminderen, in tegenstelling tot de intentie die de wetgever in de NIS2-wet zelf heeft uitgedrukt.

35. Dit gezegd zijnde, **is de Autoriteit niet bevoegd om zich uit te spreken over de toepassing van artikel 29 van het Wetboek van Strafvordering in het kader van het project in de fase waarin het aan haar is voorgelegd met het oog op de afgifte van een machtiging.** De toepassing van deze bepaling zal in voorkomend geval leiden tot een afzonderlijke en verdere verwerking van persoonsgegevens op grond van een verplichting naar Belgisch recht, die met name moet worden beoordeeld op basis van artikel 6.4 van de AVG (verwerking op grond van het Belgische recht), buiten de machtigingsbevoegdheid van de Autoriteit om.
36. Wat betreft de **uitwisseling van informatie met de inlichtingen- en veiligheidsdiensten** zoals bedoeld in artikel **25, § 2, van de NIS2-wet**¹⁶ en artikel **20, § 1, van de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten**¹⁷, gelden de overwegingen met betrekking tot artikel 29 van het Wetboek van Strafvordering *mutatis mutandis*. De Autoriteit maakt echter uit het antwoord van de aanvrager op dat er geen ruwe elektronische-communicatiemetagegevens zullen worden uitgewisseld; wel zal: "*informatie op geaggregeerde wijze [...] verwerkt worden om trends vast te stellen*". Zij merkt terloops op dat, op basis van de adviespraktijk van de Autoriteit, de twee voornoemde bepalingen *op zichzelf*, overeenkomstig de beginselen van voorspelbaarheid en rechtmatigheid zoals vastgelegd in artikel 8 van het EVRM en artikel 22 van de Grondwet, geen verwerking van persoonsgegevens kunnen rechtvaardigen. Zij wijst de aanvrager nogmaals op het feit dat, ook al zijn bepaalde gegevens vanuit zijn oogpunt geen persoonsgegevens, het doorgeven ervan aan een ontvanger voor wie deze gegevens wel persoonsgegevens kunnen zijn, op zich wel degelijk een verwerking van persoonsgegevens vormt¹⁸.

¹⁶ Deze bepaling luidt als volgt:

"Naargelang de behoeften die nodig zijn voor de uitvoering van deze wet werken de in paragraaf 1 bedoelde autoriteiten op nationaal niveau ook samen met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening (EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de wet van 1 juli 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten."

¹⁷ Deze bepaling luidt als volgt:

"De inlichtingen- en veiligheidsdiensten, de politiediensten, de administratieve en gerechtelijke overheden zorgen voor een zo doeltreffend mogelijke wederzijdse samenwerking. De inlichtingen- en veiligheidsdiensten zorgen er eveneens voor dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten."

¹⁸ Zie in dit verband het arrest van het Hof van Justitie van de Europese Unie van 9 november 2023, *Gesamtverband Autoteile-Handel eV tegen Scania CV AB*, zaak C-319/22, punten 48-49:

"Gelet daarop vormt het VIN een persoonsgegeven in de zin van artikel 4, punt 1, AVG van de natuurlijke persoon die op hetzelfde kentekenbewijs is vermeld, voor zover degene die er toegang toe heeft over de middelen kan beschikken om het redelijkerwijs in te zetten voor de identificatie van de eigenaar van het voertuig of van een persoon die in een andere juridische hoedanigheid dan die van eigenaar over het betrokken voertuig kan beschikken."

Met name wat betreft de elementen die in overweging moeten worden genomen om te bepalen of gegevens voor een ontvanger persoonsgegevens kunnen zijn, moet ook rekening worden gehouden met de wettelijke kanalen waarover deze beschikt om aanvullende informatie van derden te verkrijgen¹⁹.

37. Dit gezegd zijnde, is de **Autoriteit**, nogmaals, **in de fase waarin de zaak aan haar wordt voorgelegd met het oog op de afgifte van een machtiging, niet bevoegd om zich uit te spreken over de toepassing van eventuele wettelijke verplichtingen van het CCB (nationaal CSIRT) om gegevens met betrekking tot het project aan de inlichtingen- en veiligheidsdiensten te verstrekken**. In voorkomend geval valt deze afzonderlijke en latere verwerking van persoonsgegevens op grond van een verplichting uit het Belgische recht die met name op basis van artikel 6.4 van de AVG moet worden beoordeeld (verwerking op grond van het Belgische recht), buiten de machtigingsbevoegdheid van de Autoriteit.

II.5. Gebruik van alternatieve maatregelen om op te treden tegen C2-servers

38. De aanvrager motiveert in de projectnota waarom de alternatieven voor het verzamelen van metagegevens, die de Autoriteit in haar machtiging nr. 001/2025 heeft genoemd, niet in aanmerking worden genomen. Deze overwegingen moeten in verband worden gebracht met de overwegingen 74 tot en met 78 van machtiging nr. 001/2025.
39. Vooreerst en in wezen herhaalt de aanvrager de **beperkingen van de bevoegdheden van het CCB (nationaal CSIRT)** en benadrukt hij dat hij geen zeggenschap heeft over de **gerechtelijke gevolgen** met betrekking tot mededelingen op grond van artikel 29 van het Wetboek van Strafvordering²⁰. Hoewel het inderdaad duidelijk is dat het aan de gerechtelijke autoriteit is om het

Zoals de advocaat-generaal in de punten 34 en 41 van zijn conclusie heeft opgemerkt, vormt het VIN, wanneer de onafhankelijke marktdeelnemers redelijkerwijs kunnen beschikken over middelen waarmee een VIN kan worden gekoppeld aan een geïdentificeerde of identificeerbare natuurlijke persoon, hetgeen de verwijzende rechter dient te verifiëren, voor deze marktdeelnemers een persoonsgegeven in de zin van artikel 4, punt 1, AVG, en is het VIN dit ook indirect voor de autofabrikanten die het ter beschikking stellen, ook al is het VIN op zich voor laatstgenoemden geen persoonsgegeven en is het dat niet met name wanneer het voertuig waaraan dit VIN is toegekend niet aan een natuurlijke persoon toebehoort." (in vet aangeduid door de Autoriteit)

Meer recentelijk overgenomen in het arrest van het Hof van Justitie van de Europese Unie (Eerste kamer) van 4 september 2025, *EDPS tegen GAR* (of "SRB"), zaak C-413/23, paragraaf 84.

¹⁹ HvJ-EU (2e kamer), arrest van 19 oktober 2016, *Breyer*, zaak C-582/14, punten 43-48; HvJ-EU (4e kamer), arrest van 7 maart 2024, *IAB Europe tegen Gegevensbeschermingsautoriteit*, zaak C-604/22, punt 48.

²⁰ Meer bepaald:



Krachtens artikel 29 van het Strafwetboek is elke ambtenaar die bij de uitoefening van zijn functie kennis krijgt van een misdrijf of een overtreding, verplicht om de procureur des Konings hiervan onmiddellijk op de hoogte te brengen en hem de desbetreffende informatie door te geven. We kunnen echter geen uitspraak doen over wat er gebeurt met dergelijke aangiften bij het openbaar ministerie (dat volledig onafhankelijk en volgens zijn eigen prioriteiten handelt), laat staan over de beslissing om IP-adressen al dan niet te blokkeren/filteren of de gerechtelijke autoriteiten in te schakelen om IP-adressen van C2-servers te filteren/blokkeren (bijv. art. 39bis, § 1, Strafwetboek)." (in vet aangeduide tekst door de Autoriteit weggelaten).

beleid te bepalen dat zij op dit gebied wil voeren, zoals de Autoriteit aangeeft in overweging 76 van haar machtiging nr. 001/2025, *"blijft de mededeling aan de gerechtelijke autoriteiten van de in het kader van het project vastgestelde ongeoorloofde activiteiten van C2-servers in ieder geval relevant, en kan het strafrechtelijk beleid ter zake bovendien evolueren"*.

40. Wat vervolgens de **vrijwillige filtering door de operatoren** betreft, geeft de aanvrager aan dat ■ (vetgedrukt weggelaten door de Autoriteit). Dit geeft aanleiding tot de volgende twee opmerkingen.
41. Ten eerste herinnert de Autoriteit eraan, zonder hier nader in te gaan op wat de operatoren in voorkomend geval in de contractuele voorwaarden van hun diensten opnemen, dat zij ook **wettelijke verplichtingen hebben met betrekking tot de veiligheid van hun diensten**. Ze zijn met name verplicht om op te treden in geval van een *"ernstige cyberdreiging"* en het BIPT kan in dit kader zelf bindende instructies geven aan de verstrekkers van digitale infrastructuur²¹. Het project is echter duidelijk gericht op het afweren van ernstige bedreigingen. Bovendien bepaalt artikel 121/8, § 1, van de WEC het volgende: *"Zonder kennis te nemen van de inhoud van de communicatie, treffen de operatoren de gepaste, evenredige, preventieve en curatieve maatregelen, rekening houdende met de meest recente technische mogelijkheden, om fraude en kwaadwillig gebruik op hun netwerken en diensten op te sporen en om te vermijden dat de eindgebruikers schade lijden of lastiggevallen worden."*
42. Ten tweede kan in principe niet worden uitgesloten dat het blokkeren van een IP-adres door een operator nooit kan worden uitgevoerd en nooit doeltreffend zal zijn om zijn klanten te beschermen. Met andere woorden **is het niet uitgesloten dat de benadering van het project, op een bepaald moment en/of in bepaalde gevallen, kan worden gecombineerd met het filteren/blokkeren door de operatoren.** ■
43. Ten slotte, en dit is **het doorslaggevende punt dat door de aanvrager werd aangevoerd** en dat de Autoriteit ertoe heeft gebracht het **in het kader van diens project ingediende verzoek om toegang goed te keuren in plaats van het gebruik van alternatieve methoden op te leggen waarbij geen elektronische-communicatiemetagegevens worden verwerkt**, stelt de aanvrager dat ■ (vetgedrukt gewijzigd door de Autoriteit).
44. Het is *in fine* en *in concreto* dus aan het CCB (nationaal CSIRT) om, in het kader van zijn wettelijke opdracht en met gebruikmaking van de speelruimte waarover het daartoe beschikt, te beoordelen of en wanneer een alternatieve blokkerings- of filtermaatregel door een derde nuttig zou kunnen zijn, teneinde het hoogste veiligheidsniveau te waarborgen, rekening houdend met het beleid dat het op

²¹ Zie de artikelen 107/2 tot en met 107/5 van de WEC.

dit gebied voert. **De Autoriteit vraagt om deze mogelijkheid in overweging te nemen** en deze niet systematisch in alle gevallen van de hand te wijzen. Met dien verstande dat de Autoriteit in dit verband wel degelijk kennis heeft genomen van het feit dat de juridische bevoegdheid om een dergelijke maatregel op te leggen, *ontbrak*.

45. **Deze overwegingen doen echter geen afbreuk aan het nut van het gebruik van Threat Alerts, zoals bedoeld in de overwegingen 79 tot en met 81 van machtiging nr. 001/2025.**

In zijn projectnota preciseert de aanvrager het volgende:

*"De dienst Cyber Threat Alerts biedt algemene of gerichte informatie aan organisaties (NIS2 entiteiten of niet) **die zich hebben geregistreerd op het SafeOnWeb@Work platform van het CCB en die deze dienst hebben geactiveerd.***

■

*Het doel is om deze slachtoffers in staat te stellen zich te beschermen tegen kwaadwillige activiteiten die via deze C2-servers worden uitgevoerd. **Het doel van het CCB is vervolgens om uitsluitend de slachtoffers van een C2-server specifiek te informeren. Dit is vaak niet mogelijk via Cyber Threat Alerts,*** ■

De dienst Cyber Threat Alerts alleen volstaat dus niet om de slachtoffers van deze C2-servers te identificeren en te informeren.

■ (in vet aangeduid door de Autoriteit).

46. Hoewel de Autoriteit zich ervan bewust is dat Threat Alerts niet volstaat om het door de aanvrager nagestreefde doel te bereiken, heeft zij de aanvrager niettemin gevraagd of dit kanaal ook wordt gebruikt om te communiceren over de geïdentificeerde C2-servers. Hij antwoordde het volgende (vrije vertaling):

■

47. De Autoriteit maakt uit dit antwoord op dat Threat Alerts momenteel dus **niet** wordt gebruikt om op algemene wijze informatie over C2-servers te verspreiden. Ook hier is de Autoriteit van mening dat het aan het CCB (nationaal CSIRT) is **om na te gaan of ook dit informatiekanaal kan worden gebruikt** om passende informatie te verspreiden (wel of niet te nemen preventieve maatregelen, enz.) over de betrokken C2-servers en IP-adressen. ■

II.6. Controle of een IP-adres wel degelijk uitsluitend bestemd is en blijft voor de activiteiten van een C2-server

II.6.1. Uitgevoerde controles

48. In het kader van de aanvraag heeft de Autoriteit de aanvrager opnieuw gevraagd naar de controlemaatregelen die zijn genomen om vast te stellen dat de betreffende IP-adressen bestemd zijn en blijven voor het verkeer van C2-servers.

49. ■

50. De Autoriteit neemt kennis van de maatregelen die door het CCB (nationaal CSIRT) zijn genomen ■ Deze maatregelen, die passend zijn, vragen geen aanvullende opmerkingen van de Autoriteit. Dit gezegd zijnde, hoewel de Autoriteit begrijpt dat inderdaad, ■ een administratieve last met zich meebrengt die vertragend kan werken en bijgevolg de doeltreffende uitvoering van het ontwerp kan schaden, **is het niettemin de taak van het CCB (nationaal CSIRT) om hiervan minimaal een spoor bij te houden in een vorm naar eigen keuze, in het kader van zijn accountability-plicht** ■

51. Bovendien heeft de Autoriteit de aanvrager ook gevraagd hoe hij vaststelt ■ Hij antwoordde het volgende:

■
■

52. De Autoriteit neemt kennis van deze toelichtingen en van de door het CCB (nationaal CSIRT) gevolgde passende methode, die geen aanvullende opmerkingen van de Autoriteit vereist. Wanneer het CCB (nationaal CSIRT) zijn analyse op deze manier onderbouwt, dient te worden **aangegeven op welke bronnen het zich heeft gebaseerd.**

II.6.2. Wijziging van de controlefrequentie van IP-adressen

53. In haar projectnota past het CCB (nationaal CSIRT) de controlefrequentie van de geregistreerde IP-adressen aan om te waarborgen dat deze daadwerkelijk bestemd blijven voor het verkeer van een C2-server. Ter herinnering, **er werd overwogen** om deze adressen **dagelijks te controleren** (overwegingen 64 en 65 van machtiging nr. 001/2025). In deze nota wordt **het volgende** uitgelegd:

"De lijsten met C2-servers die aan de ISP's worden doorgegeven, moeten regelmatig worden bijgewerkt. Elk IP-adres op de lijst mag alleen op de lijst blijven staan als het nog steeds een C2-server betreft.

■
■
■
■

(vetgedrukt gewijzigd en onderstreping toegevoegd door de Autoriteit).

54. Onder deze omstandigheden moet de aanpak die in het kader van machtiging nr. 001/2025 is gekozen, worden aangepast. Het ontwerp vereist de invoering van een **efficiënt controleproces, dat ten minste wekelijks en, indien gerechtvaardigd, frequenter plaatsvindt, om na te gaan of elk betrokken IP-adres nog steeds relevant is** voor het project (controle of het adres nog steeds uitsluitend wordt gebruikt voor de activiteiten van een C2-server), **op basis van de controlemaatregelen zoals bedoeld in de overwegingen 57 en 59 van machtiging nr. 001/2025** (zie ook de overwegingen 49-51 van deze machtiging), **waarbij het CCB, in het kader van zijn *accountability*-plicht, een spoor moet bijhouden van de rechtvaardiging van de gekozen periodiciteit** ■

II.7. Beperking van de contextuele informatie die aan de operatoren wordt verstrekt

55. Wat betreft het verstrekken van contextuele informatie aan operatoren, zodat deze aan hun eigen verplichtingen inzake gegevensbescherming kunnen voldoen, verduidelijkt de aanvrager het volgende in zijn projectnota:

*"Wat betreft de informatie die het CCB aan de elektronische-communicatie-operator moet verstrekken bij een toegangsverzoek, dient te worden opgemerkt dat **artikel 127/1, § 6 van de WEC**^[22] **niet vereist dat de operator de precieze contextuele informatie met betrekking tot het verzoek wordt verstrekt,** ■*

*Bovendien **moet het CCB, overeenkomstig artikel 26, § 3 van de NIS2-wet, de toegang tot informatie, met name dergelijke gevoelige informatie, strikt beperken tot personen die deze informatie nodig hebben en er toegang toe moeten hebben***

²² Deze bepaling luidt als volgt:

"De verzoeken die de autoriteiten richten aan de operatoren om bepaalde gegevens te verkrijgen die worden bewaard krachtens de artikelen 122, 123, 126, 126/1, 126/3 of 127, omvatten de volgende minimale vermeldingen:

1° de identiteit van de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de identiteit van die dienst;

2° de functie van de contactpersoon bij de verzoekende autoriteit, of, wanneer het verzoek naar de operator verzonden wordt door een centrale dienst voor rekening van die autoriteit, de functie van de contactpersoon bij die centrale dienst;

3° de juridische grondslag waarop het verzoek gebaseerd is, behalve wanneer het verzoek naar de operator wordt verzonden via een centrale dienst voor rekening van een andere autoriteit;

4° de gewenste antwoordtermijn".

voor de uitoefening van hun taken of hun opdracht in verband met de uitvoering van deze wet.



Alle documenten die door het CCB in het kader van dit project worden geproduceerd, zijn geclassificeerd als "GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)" - TLP:AMBER+STRICT" (in vet aangeduid en onderstreept door de Autoriteit).

56. Het klopt dat artikel 127/1 van de WEC niet expliciet betrekking heeft op de verstrekking van alle contextuele informatie door het CCB (nationaal CSIRT) aan de operatoren zoals bedoeld door de Autoriteit in haar machtiging nr. 001/2025, en dat artikel 26, § 3, van de NIS2-wet het CCB verplicht om de toegang tot informatie in het kader van deze wet te beperken tot de personen die deze informatie nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun taken of opdracht ter uitvoering ervan.
57. Ten eerste **geeft** de aanvrager echter **niet aan** (en ziet de Autoriteit evenmin in) **waarom het verstrekken van contextuele informatie aan de operatoren** die belast zijn met het verzamelen en doorgeven van elektronische-communicatiemetagegevens, **nadelig zou zijn** voor het project van de aanvrager en/of de NIS2-entiteiten. In dit verband moet overigens worden opgemerkt en toegevoegd dat **het project van de aanvrager niet alleen betrekking heeft op de NIS2-entiteiten** (alle potentiële slachtoffers zijn hierbij betrokken).
58. In ieder geval, ten tweede, **moet de operator bepaalde informatie kennen** wanneer hij tot medewerking verplicht is. In dit verband **voorziet** het **normatieve kader** dat van toepassing is op het verzoek van de operatoren om elektronische-communicatiemetagegevens te verkrijgen **met name in de invoering van specifieke technische en organisatorische maatregelen**²³. En bepaalde betrokken contextuele gegevens kunnen zelfs **openbaar** zijn (dit geldt bijvoorbeeld voor het **land van herkomst** van het IP-adres²⁴).
59. Ten derde zijn zowel het CCB (nationaal CSIRT) als de betrokken operator verwerkingsverantwoordelijken en moeten zij, krachtens de **artikelen 5, 2 en 24, van de AVG**, kunnen aantonen dat de verwerkingen die onder hun respectieve verantwoordelijkheden vallen, in overeenstemming zijn met de AVG (*accountability*-beginsel). De operator moet ervoor zorgen dat de

²³ Zie overweging 89 van machtiging nr. 001/2025 en, in een gevoeliger domein, overweging 68 van advies nr. 118/2025 van 12 november 2025 *met betrekking tot een ontwerp van koninklijk besluit houdende de regels voor de vernietiging van onwettig verkregen gegevens als bedoeld in artikel 44/4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en houdende de regels voor samenwerking als bedoeld in artikel 44/5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (CO-A-2025-104).*

²⁴ De aanvrager heeft zelf herinnerd aan het volgende: "De IP-bereiken worden per land toegekend." ■

metagegevens die hij verstrekt, daadwerkelijk aansluiten bij het doeleinde van het project van de aanvrager.

60. Ten vierde voorziet artikel 127/1, § 6, van de WEC in de "**minimale**" vermeldingen die in het verzoek om metagegevens moeten worden opgenomen. Deze bepaling maakt het dus mogelijk om rekening te houden enerzijds met het feit dat de WEC moet worden gecombineerd met specifieke wetgeving die de toegang tot metagegevens regelt (zoals in dit geval de NIS2-wet), waarbij in voorkomend geval in andere aanvullende vermeldingen kan worden voorzien, en anderzijds, volgens de Autoriteit, met de uitvoering van andere wettelijke verplichtingen, zoals het zojuist genoemde *accountability*-beginsel.
61. Hieruit volgt dat de aanvrager in de verzoeken aan de operatoren **per IP-adres** ten minste het volgende moet vermelden: het **land van herkomst** van het betrokken IP-adres, alsook de **concrete bedreiging/kwaadwillige activiteit** (ransomware, spionage, enz.) **die voor België relevant is** (zie in dit verband de overwegingen 56 en 58 van machtiging nr. 001/2025).

II.8. Bewaartermijn van de gegevens

62. De Autoriteit heeft de aanvrager opnieuw gevraagd naar de rechtvaardiging van een bewaartermijn van één jaar voor de verzamelde metagegevens, aangezien, zodra de benaderde potentiële slachtoffers een redelijke termijn hebben gehad om zich te beraden over de verwerking van de gegevens (en in voorkomend geval contact op te nemen met de verwerkingsverantwoordelijke), de noodzaak om de gegevens gedurende deze periode te bewaren niet zo vanzelfsprekend is. De Autoriteit stelde zich met name vragen bij het volgende doeleinde dat in de documentatie wordt genoemd: "***zodat de informatie tussen de activiteiten van de verschillende C2-servers (analyse van de dreiging en de ontwikkeling ervan in de tijd) op zinvolle wijze kan worden gekoppeld.***" (in vet aangeduid door de Autoriteit) Om welke koppelingen gaat het precies en hoe sluiten deze aan bij het doeleinde dat het project van de aanvrager nastreeft; kunnen deze niet op basis van geaggregeerde of geanonimiseerde gegevens worden gerealiseerd? De aanvrager antwoordde het volgende:

■
■

Dit kan inderdaad gebeuren op basis van geaggregeerde en geanonimiseerde gegevens. ■ (in vet aangeduid en onderstreept door de Autoriteit).

63. De Autoriteit is van mening dat de verwerking van de gegevensanalyse zoals beschreven in het antwoord van de aanvrager, met het oog op het identificeren van ■ **een verdere gegevensverwerking vormt die verenigbaar is met het oorspronkelijke doeleinde van het project, hetgeen rechtvaardigt dat de verzamelde metagegevens worden bewaard gedurende een periode van één jaar vanaf het moment van verzameling, ondanks het feit**

dat een dergelijke gegevensbewaring niet noodzakelijk is om de slachtoffers van de C2-servers te waarschuwen. Hoewel de betrokken analyses op zich niet noodzakelijk zijn om potentiële slachtoffers te identificeren en te informeren, zijn ze wel **nodig om de methoden van het CCB (nationaal CSIRT) te perfectioneren en aan te passen**, teneinde de C2-servers, hun potentiële slachtoffers en de door hen te ondernemen stappen te identificeren, en zelfs in het algemeen maatregelen te nemen tegen de betrokken C2-servers.

64. Dit gezegd zijnde, **moeten** deze analyses, **overeenkomstig het beginsel van minimale gegevensverwerking, worden uitgevoerd op basis van geanonimiseerde gegevens en bij gebrek daaraan, indien dit in de praktijk onmogelijk blijkt** (wat overeenkomstig het *accountability*-beginsel moet worden gedocumenteerd), **op basis van geaggregeerde gegevens.**

II.9. Rechten van de betrokkenen

65. In de context van machtiging nr. 001/2025 (overwegingen 99-102) gaf de aanvrager aan dat de rechten van de betrokkenen in het kader van zijn project **niet werden beperkt**. De **documentatie bevestigt dat de rechten van de betrokkenen in het kader van het project van toepassing zijn.**
66. Hierin roept het volgende uittreksel echter vragen op: "*Het CCB is verplicht om, voor zover mogelijk, de betrokken natuurlijke personen te informeren over de toegang tot hun elektronische communicatiegegevens **wanneer dit het goede verloop van zijn taken of een lopend onderzoek niet meer in gevaar brengt** en wanneer deze personen kunnen worden geïdentificeerd.*" (in vet aangeduid door de Autoriteit) De Autoriteit heeft de aanvrager gevraagd aan te geven welke gevallen worden bedoeld en wat de wettelijke grondslag hiervoor is. Hij antwoordde het volgende (vrije vertaling):



Deze beperking is gebaseerd op artikel 21, § 6, van de NIS2-wet, waarin staat: "Het nationale CSIRT brengt de betrokken natuurlijke personen voor zover mogelijk op de hoogte van de toegang tot hun elektronische-communicatiegegevens als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd" (door ons onderstreept). Onder "zijn taken" moeten de taken worden verstaan waarnaar in paragraaf 2 van hetzelfde artikel 21 wordt verwezen, namelijk deze die zijn opgesomd in artikel 19, § 1, [eerste lid,] 1° tot en met 5°, van dezelfde wet, waaronder de volgende taak: "het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en

belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk”.

67. Artikel 21, § 6, van de NIS2-wet regelt weliswaar een verplichting om de betrokkenen te informeren²⁵, maar voorziet niet in een afwijking van het recht op inzage van de betrokkenen. In ieder geval is ofwel de betrokkene zelf een potentieel slachtoffer van de betreffende C2-server. In dat geval ontvangt deze een kennisgeving van het CCB (nationaal CSIRT) en wordt hij dus noodzakelijkerwijs op de hoogte gebracht van de voorafgaande gegevensverzameling en van de stappen die al dan niet moeten worden ondernomen, overeenkomstig het project. Ofwel zijn de analyses nog gaande, waardoor de status van de betrokkene nog niet vaststaat, hij nog niet is geïdentificeerd en nog niet op de hoogte kan worden gebracht. Het CCB (nationaal CSIRT) kan hem dus nog niet informeren en indien hij zijn recht van inzage uitoefent, is artikel 11 van de AVG van toepassing. Hetzelfde geldt indien het IP-adres van de betrokkene niet wordt beschouwd als dat van een potentieel slachtoffer. Mocht de betrokkene echter aan de hand van bewijskrachtige documenten aantonen welk(e) IP-adres(sen) hem gedurende één of meer bepaalde periodes is/zijn toegewezen, dan zou zijn verzoek op grond van het recht van inzage niettemin ontvankelijk zijn.

68. Dit gezegd zijnde, **is de Autoriteit op het moment dat de zaak aan haar wordt voorgelegd met het oog op de afgifte van een machtiging, niet bevoegd om zich uit te spreken over de toepassing van de rechten van de betrokkenen in het kader van het project.**

II.10. Wettelijke grondslag voor de verwerking en wijziging van het bestaande normatieve kader

69. In haar machtiging nr. 001/2025 wees de Autoriteit de aanvrager erop dat het van belang is dat de wetgever de reikwijdte bevestigt die de Autoriteit in diezelfde machtiging aan de NIS2-wet heeft toegekend (rekening houdend met het verkeer van entiteiten die niet onder NIS2 vallen, met inbegrip van natuurlijke personen). In het kader van de onderhavige aanvraag heeft de aanvrager de Autoriteit gewezen op amendement nr. 12 op een wetsontwerp *betreffende de weerbaarheid van kritieke entiteiten*²⁶, dat artikel 5 van de NIS2-wet aanvult met een paragraaf 7 die als volgt luidt: “*De artikelen 8 en 38, evenals de bepalingen van titel 2, worden aldus uitgelegd dat ze van toepassing zijn op elke natuurlijke of rechtspersoon die in België aanwezig of gevestigd is.*” In het kader van de voorbereiding van het onderhavige machtigingsdossier heeft de Autoriteit de aanvrager ondervraagd, waarna deze heeft aangegeven dat er (naar aanleiding van het advies van de Raad van State) een interpretatieve

²⁵ Dit “lid [bepaalt] dat het CSIRT de betrokken natuurlijke personen voor zover mogelijk op de hoogte moet brengen van de toegang tot hun elektronische-communicatiegegevens, als de uitvoering van zijn taken of van een lopend onderzoek hierdoor niet meer in het gedrang kan komen en als deze personen kunnen worden geïdentificeerd. Deze bepaling beoogt uitvoering te geven aan de beginselen van transparantie en voorlichting van de betrokkenen, voor zover dit geen afbreuk doet aan lopende acties.”, *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 55-2572/001, p. 173.

²⁶ *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 56-1002/002, p. 16.

bepaling was voorgesteld, en dat deze *"op 18 december 2025 samen met het gehele CER-wetsontwerp door de Kamer van volksvertegenwoordigers is aangenomen. We wachten op de publicatie en de inwerkingtreding van deze wet. Volgens de informatie waarover wij beschikken, zal de CER-wet binnenkort worden gepubliceerd onder de datum van de wet van 19 december 2025."* (vrije vertaling)

70. De Autoriteit **analyseert de inmiddels aangenomen bepaling niet en beperkt zich, met betrekking tot de aanvraag, tot de volgende opmerking.**

71. In het algemeen heeft de Autoriteit nooit betwist dat de NIS2-wet in een hele reeks gevallen wel degelijk van toepassing kan zijn op natuurlijke personen en de verwerking van persoonsgegevens met betrekking tot deze personen kan inhouden, met inbegrip van gegevens uit elektronische communicatie. Overigens *in fine*, op het gebied van elektronische communicatie, zelfs wanneer de abonnee van de betrokken elektronische communicatiedienst een rechtspersoon is (bv. een NIS2-entiteit), kunnen de concrete deelnemers aan de elektronische communicatie natuurlijke personen²⁷ zijn, die bovendien gemakkelijk identificeerbaar zijn door de betrokken rechtspersoon, die in principe een logboek bijhoudt van het gebruik van zijn privénetwerk²⁸. Met andere woorden, vanaf het begin was het duidelijk niet uitgesloten dat de toepassing van het project van de aanvrager, zelfs indien deze beperkt tot het verkeer van uitsluitend NIS2-entiteiten, *in concreto* betrekking zou kunnen hebben op natuurlijke personen en de verwerking van hun persoonsgegevens²⁹.

72. De bezorgdheid die de Autoriteit uitte, was specifiek van aard. Het betrof het feit dat het project zou kunnen inhouden dat er op het niveau van de operatoren in zekere mate realtime monitoring plaatsvindt van het IP-verkeer van entiteiten die geen NIS2-entiteiten zijn, namelijk onder meer entiteiten (met inbegrip van natuurlijke personen) die, gezien hun doeleinden, niet de eerste en belangrijkste doelgroep zijn van de Europese en Belgische NIS2 normatieve bepalingen. Dit is een vraagstuk dat overigens in het licht moet worden gezien van de netwerkmonitoring die in de nationale strategie op het gebied van cyberveiligheid wordt overwogen³⁰. Zonder al te diep op dit onderwerp in te gaan, kunnen we het volgende opmerken. Het verzamelen van persoonsgegevens in het kader van een concrete interventie naar aanleiding van een beveiligingsincident dat een persoon heeft getroffen en de proactieve monitoring in realtime van het IP-verkeer op het niveau van de operatoren zijn verschillende vormen van gegevensverwerking en benadering (reactief of proactief) die niet dezelfde

²⁷ Dit zijn de natuurlijke personen die daadwerkelijk gebruikmaken van de betreffende dienst.

²⁸ Zie overwegingen 31 en 101 van machtiging nr. 001/2025.

²⁹ Ook bij de C2-server zullen op de een of andere manier één of meer natuurlijke personen betrokken zijn (bv. een crimineel of een vertegenwoordiger van een vijandige staat). Het is trouwens in theorie niet uitgesloten dat het betrokken IP-adres zich in het buitenland bevindt en rechtstreeks aan een natuurlijke persoon kan worden gekoppeld. Dit had geen enkele invloed op de rechtmatigheid of het normatieve kader van een project van de aanvrager dat uitsluitend beperkt zou zijn gebleven tot het monitoren van het verkeer van NIS2-entiteiten.

³⁰ Zie over dit punt advies nr. 69/2025 van de Autoriteit *met betrekking tot de "Nationale Cybersecurity Strategie 3.0, 2026-2030" (CO-A-2025-108)*, overwegingen 11-15.

mate van inmenging in de rechten en vrijheden van personen inhouden. Bijgevolg kunnen zij minder of juist meer precieze en gedetailleerde normatieve kaders vereisen, overeenkomstig artikel 22 van de Grondwet, artikel 8 van het EVRM en de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie. In dit verband heeft de Autoriteit herinnerd aan de grenzen van haar tussenkomst in het kader van een machtiging en aan de noodzaak dat de wetgever zelf de essentiële elementen vaststelt van de gegevensverwerkingen die hij voornemens is uit te voeren³¹.

73. Dit gezegd zijnde, neemt de Autoriteit nota van de stappen die op dit gebied zijn ondernomen.

II.11. Beslissing

De Autoriteit beslist, binnen de grenzen zoals vermeld in de overwegingen 12-17 van machtiging nr. 001/2025 en in de overwegingen 6-9, het volgende:

1. De aanvrager moet de Autoriteit binnen de 10 werkdagen vanaf de kennisgeving van deze beslissing (de datum van verzending van de e-mail van de Autoriteit aan de aanvrager geldt als bewijs) duidelijk aangeven welke passages van haar beslissing volgens hem niet mogen worden gepubliceerd om de door hem aangevoerde redenen (**overwegingen 6-11 van machtiging nr. 001/2025; overwegingen 2-4**);

2. Elk concrete machtigingsaanvraag voor toegang tot elektronische-communicatiemetagegevens bij een operator moet vooraf ter goedkeuring worden voorgelegd aan de Autoriteit. Dit sluit niet uit dat daaropvolgende aanvragen tot machtiging of controle achteraf in dringende gevallen kunnen verwijzen naar de onderhavige beslissing en naar machtiging nr. 001/2025, mits zij verder uitvoerig gemotiveerd blijven.

De Autoriteit staat positief tegenover de gevolgde aanpak van de aanvrager om, gezien de wijzigingen in zijn project, een voorafgaande machtigingsaanvraag in te dienen, in plaats van - ervan uitgaande dat in het kader van zijn aanvraag een beroep op dringendheid zou kunnen worden gedaan - de Autoriteit voor een voldongen feit te plaatsen in een situatie van controle achteraf. Een dergelijke benadering garandeert een efficiëntere en juridisch gezien veiligere werkwijze. Zij verwacht van de aanvrager dat hij in de toekomst duidelijk aangeeft welke overwegingen in zijn beslissingen moeten worden aangepast als gevolg van de wijziging van het project (**overwegingen 18-24 van machtiging nr. 001/2025; overwegingen nr. 6-7**);

³¹ Zie overwegingen 14 en 15 van machtiging nr. 001/2025.

3. De Autoriteit is niet bevoegd om vragen te behandelen die verband houden met de vrijwillige uitwisseling van gegevens tussen de operator en het CCB (nationaal CSIRT) in het kader van de machtigingsaanvraag waarop de onderhavige beslissing betrekking heeft, en zeker niet om zich uit te spreken over een dergelijk scenario van gegevensverwerking, aangezien dit buiten het toepassingsgebied valt van artikel 21, § 2, van de NIS2-wet (**overwegingen 11-14**);

4. Het ontwerp steunt op artikel 19, § 1, 2°, van de NIS2-wet. Het betreft het verspreiden van meldingen en informatie over cyberdreigingen en kwetsbaarheden onder de betrokken entiteiten en personen die potentieel slachtoffer zijn, nadat de daarvoor nodige analyse- en opsporingswerkzaamheden zijn uitgevoerd (**overwegingen 25-29 van machtiging nr. 001/2025**) (**overwegingen 29-31**);

5. In elke voorafgaande machtigingsaanvraag moet(en) de operator(en) worden vermeld waarop de machtigingsaanvraag betrekking heeft (**overwegingen 33-36 van machtiging nr. 001/2025**). Machtiging voor toegang tot de hieronder genoemde metagegevens is toegestaan bij Belnet, Proximus en Telenet (**overwegingen 17-18**);

6. De metagegevens met betrekking tot elektronische-communicatiemetagegevens voorafgaand aan de datum van deze beslissing mogen alleen worden verzameld op basis van de door het CCB (nationaal CSIRT) vastgestelde "*first seen*"-datums (zie de methodenota en bijlage 1) indien aan de volgende vier voorwaarden is voldaan (**overwegingen 19-28**):

- De metagegevens worden verzameld op basis van precieze wettelijke grondslagen (artikel en naargelang het geval, paragraaf, lid, punt en nummer) die expliciet en duidelijk door het CCB (nationaal CSIRT) aan de operatoren worden aangegeven (het CCB nationaal CSIRT mag zich op dit punt niet beperken tot een algemene verwijzing naar de artikelen 122 en 123 van de WEC);
- De metagegevens worden door de betrokken operatoren wettelijk bewaard, overeenkomstig de artikelen 122 en 123 van de WEC, afhankelijk van de wettelijke grondslag van de aanvraag;
- De aanvrager zet een procedure op om in het kader van zijn project direct rekening te houden met de verwachte uitspraak van het Hof van Justitie: hij moet de rechtmatigheid van de verwerking van metagegevens in het kader van het project op basis van die uitspraak opnieuw beoordelen en daaruit de nodige conclusies trekken;

- Elke bijgehouden “*first seen*”-datum wordt in de door de aanvrager bewaarde documentatie gekoppeld aan een concrete gebeurtenis die wijst op een verband tussen de betrokken activiteit van de C2-server waarop de aanvraag betrekking heeft en het betrokken IP-adres. Indien deze datum te ver in het verleden ligt met betrekking tot de wettelijk toegestane bewaartermijnen voor metagegevens door de operatoren, moet de datum van de metagegevens die mogen worden verzameld dienovereenkomstig worden aangepast in de documentatie van de aanvrager.

7. Het project kan betrekking hebben op de elektronische-communicatiemetagegevens tussen de C2-servers en de essentiële of belangrijke entiteiten waarop de NIS2-wet van toepassing is, alsook op de elektronische-communicatiemetagegevens tussen deze C2-servers en andere entiteiten, met inbegrip van natuurlijke personen (**overwegingen 37-44 van machtiging 001/2025**). De Autoriteit neemt kennis van de stappen die door de aanvrager zijn ondernomen, alsook van het feit dat er een interpretatieve bepaling met betrekking tot de NIS2-wet is aangenomen. De bezorgdheid die de Autoriteit in haar machtiging nr. 001/2025 uitte, betrof het feit dat het project zou kunnen inhouden dat er op het niveau van de operatoren in zekere mate realtime monitoring plaatsvindt van het IP-verkeer van entiteiten die geen NIS2-entiteiten zijn, namelijk onder meer entiteiten (met inbegrip van natuurlijke personen) die, gezien hun doeleinden, niet de eerste en belangrijkste doelgroep zijn van de Europese en Belgische NIS2 normatieve bepalingen (**overwegingen 69-73**);

8. De identificatie van een slachtoffer gebeurt op basis van verschillende elementen: ■ (**overwegingen 46-50 van machtiging nr. 001/2025**);

9. De verzameling van identificatiebronnen van IP-adressen die door de aanvrager worden vermeld in het kader van het project, moet in overeenstemming zijn met de NIS2-wet. Bovendien vereist het project de invoering van een doeltreffend proces voor de controle van de kwaliteit van de informatie over C2-servers die door al deze bronnen wordt verstrekt, en dus ook van het feit dat de betrokken IP-adressen daadwerkelijk bestemd zijn voor het verkeer van C2-servers die zijn geselecteerd op basis van de ernst van de impact van hun activiteiten. Dit proces moet de relevante combinaties van technische maatregelen omvatten die door de aanvrager zijn meegedeeld in het kader van machtiging nr. 001/2025 en de onderhavige machtiging (**overwegingen 48-52**), evenals, indien van toepassing, alle andere aanvullende maatregelen die de stand van de techniek op dit gebied zou vereisen. Ten slotte moet de aanvrager het betrouwbaarheidsniveau van de informatiebronnen, diensten en dienstverleners waarop hij in het kader van de uitvoering van het project een beroep doet, beoordelen en aangeven. Deze processen en de uitvoering ervan moeten worden gedocumenteerd in het kader van de *accountability* (**overwegingen 52-61 van machtiging nr. 001/2025**).

10. Het ontwerp vereist de invoering van een efficiënt controleproces, dat ten minste wekelijks en, indien gerechtvaardigd, frequenter plaatsvindt, om na te gaan of elk betrokken IP-adres nog steeds relevant is voor het project (controle of het adres nog steeds uitsluitend wordt gebruikt voor de activiteiten van een C2-server), op basis van de controlemaatregelen zoals bedoeld in de overwegingen 57 en 59 van machtiging nr. 001/2025 (zie ook de overwegingen 49-51 van de onderhavige machtiging), waarbij het CCB, in het kader van zijn *accountability*-plicht, een spoor moet bijhouden van de rechtvaardiging van de gekozen periodiciteit die wordt gehanteerd in het licht van de activiteitendynamiek van de betreffende C2-server, de stand van de techniek en de relevante goede praktijken (**overwegingen 53-54**);

11. Het project vereist dat zodra het CCB (nationaal CSIRT) vaststelt dat een IP-adres niet langer gekoppeld is aan de betrokken C2-server, de betrokken operator hiervan onmiddellijk in kennis wordt gesteld via een passend kanaal en vanaf dat moment stopt met het verzamelen van metagegevens met betrekking tot het verkeer van en naar het betrokken adres. Het project moet ook voorzien in een even doeltreffende kennisgevingsprocedure, ditmaal ter attentie van het CCB (nationaal CSIRT) wanneer de betrokken operator over objectieve elementen beschikt die de juistheid van de betrokken gegevens in twijfel trekken. De Autoriteit moet op de hoogte worden gebracht van de updates die in dit verband aan de lijst van C2-servers worden aangebracht, bij de volgende machtigingsaanvraag (of controle achteraf) dat haar in het kader van het project wordt voorgelegd (**overwegingen 67-70 van machtiging nr. 001/2025**);

12. Het CCB moet, binnen de grenzen van zijn mogelijkheden en bevoegdheden, de mogelijke gelijktijdige toepassing door derden overwegen van blokkerings- en filtertechnieken door de betrokken operatoren voor de IP-adressen die aan de betreffende C2-servers zijn toegewezen, teneinde de realisatie van de betreffende dreigingen te voorkomen. Met dien verstande dat het *in fine* en *in concreto* aan het CCB (nationaal CSIRT) is om, in het kader van zijn wettelijke opdracht en met gebruikmaking van de speelruimte waarover het daartoe beschikt, te beoordelen of en wanneer een alternatieve blokkerings- of filtermaatregel door een derde nuttig kan zijn, teneinde het hoogste veiligheidsniveau te waarborgen, rekening houdend met het beleid dat het op dit gebied voert (**overwegingen 38-44**);

13. Gelet op het doeleinde ervan en overeenkomstig de beginselen van doelbinding en evenredigheid (met inbegrip van minimale gegevensverwerking) vereist het project dat – voor zover mogelijk (op basis van de informatie waarover het CCB (nationaal CSIRT) beschikt en de risico's voor de cyberveiligheid) – wordt overwogen gelijktijdig algemene informatie te verstrekken (niet alleen ter attentie van de betrokken slachtoffers) over de betrokken C2-

servers en IP-adressen via "Cyber Threat Alerts" (**overwegingen 79-81 van machtiging nr. 001/2025; overwegingen 45-47**);

14. Het CCB (Nationaal CSIRT) moet in de verzoeken aan de operatoren per IP-adres ten minste het volgende vermelden: het land van herkomst van het betrokken IP-adres, alsook de concrete bedreiging/kwaadwillige activiteit (ransomware, spionage, enz.) die voor België relevant is (zie in dit verband de overwegingen 56 en 58 van machtiging nr. 001/2025) (**overwegingen 55-61**);

15. Elke machtigingsaanvraag in het kader van het project, evenals elk verzoek om controle achteraf in geval van dringendheid, moet de bewijskrachtige documenten bevatten (zoals de methodenota (**overweging 2**); onverminderd de mogelijkheid voor de Autoriteit om bij latere aanvragen de overlegging te vragen van de documenten op basis waarvan het CCB (nationaal CSIRT) de betrokken IP-adressen identificeert die aan de C2-servers zijn toegewezen, als zijnde relevant in het kader van het ontwerp (**overwegingen 90-93 van machtiging nr. 001/2025**);

16. De Autoriteit is, in de fase waarin de zaak aan haar wordt voorgelegd met het oog op de afgifte van een machtiging, niet bevoegd om zich uit te spreken over de uitoefening door de betrokkenen van hun rechten zoals vastgelegd in de artikelen 12 tot en met 21 van de AVG. De overwegingen die hierover in deze machtiging worden uiteengezet, worden louter ter informatie verstrekt (**overwegingen 65-68**);

17. De door het CCB (nationaal CSIRT) verzamelde elektronische-communicatiemetagegevens mogen niet verder worden verwerkt voor andere doeleinden dan deze die door het project worden beoogd (**overwegingen 103-110 van machtiging nr. 001/2025**);

De Autoriteit is echter, in de fase waarin de zaak aan haar wordt voorgelegd met het oog op de afgifte van een machtiging, niet bevoegd om zich uit te spreken over de verdere verwerking van gegevens op grond van wettelijke verplichtingen die opgelegd zijn aan het CCB (nationaal CSIRT). De overwegingen die hierover in deze machtiging worden uiteengezet, worden louter ter informatie verstrekt (**overwegingen 32-37**).

18. De verzamelde metagegevens mogen worden bewaard tot het einde van het onderzoek en de waarschuwing van de slachtoffers en tot maximaal één jaar vanaf de verzameling vanwege de *accountability*. Zij kunnen ook gedurende deze periode worden bewaard om de verwerking van de gegevensanalyse uit te voeren die in het antwoord van de aanvrager is aangegeven, voor de identificatie van ■ Dit gezegd zijnde, overeenkomstig het beginsel van

minimale gegevensverwerking, moeten deze analyses worden uitgevoerd op basis van geanonimiseerde gegevens en, bij gebrek daaraan, indien dit in de praktijk onmogelijk blijkt (wat moet worden gedocumenteerd overeenkomstig het *accountability*-beginsel), op basis van geaggregeerde gegevens (**overwegingen 111-114 van machtiging nr. 001/2025; overwegingen 62-64**);

19. Onder de hierboven en in deze beslissing genoemde voorwaarden en beperkingen, met name in punt 6 betreffende de "*first seer*"-datums, is het CCB, dat optreedt als nationaal CSIRT, gemachtigd om bij de operatoren Belnet, Proximus en Telenet de volgende elektronische-communicatiemetagegevens te verzamelen: *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*, met betrekking tot elektronische communicatie van en naar de 15 IP-adressen die zijn toegewezen aan C2-servers, zoals gecontextualiseerd in de methodenota en opgenomen in bijlage 1, vanaf de "*first seer*"-datums, indien van toepassing aangepast, en dit zolang de betrokken IP-adressen aan de betrokken C2-servers zijn toegewezen;

20. Tegen deze beslissing kan beroep worden aangetekend bij de Raad van State.

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, directeur

